

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC. AND JUNIPER NETWORKS, INC.,
Petitioners,

v.

ORCKIT CORPORATION,
Patent Owner.

Case IPR2023-00554¹
U.S. Patent No. 10,652,111

PATENT OWNER'S SUR-REPLY

¹ IPR2024-00037 (Juniper Networks, Inc) has been joined with this proceeding.

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. CLAIM CONSTRUCTION.....	2
III. THE CHALLENGED CLAIMS ARE PATENTABLE	2
A. Ground 1: Lin and Swenson do not render the claims obvious.....	2
1. Lin does not teach the claimed controller.....	2
2. Swenson discloses deep flow inspection, not deep packet inspection or the claimed controller.	7
3. A POSITA would not combine/adapt Lin and Swenson to practice the claimed controller.....	11
4. Lin does not teach sending the packet to the second entity or a different entity responsive to a single criterion.....	16
B. Ground 2: Shieh and Swenson do not render the claims obvious.....	20
C. Claims 3-5.....	22
D. Claim 6.....	23
E. Claim 7.....	25
F. Claim 16.....	26
G. Claim 30.....	27
IV. CONCLUSION	28

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Arendi v. Apple</i> , 832 F.3d 1355 (Fed. Cir. 2016)	12, 27
<i>Ariosa Diagnostics v. Verinata Health, Inc.</i> , 805 F.3d 1359 (Fed. Cir. 2015)	19, 20, 24
<i>Aspex Eyewear, Inc. v. Marchon Eyewear, Inc.</i> , 672 F.3d 1335 (Fed. Cir. 2012)	25
<i>Cutsforth v. MotivePower</i> , 636 Fed.Appx. 575 (Fed. Cir. 2016).....	12
<i>DSS Tech. Mgmt. Inc. v. Apple Inc.</i> , 885 F.3d 1367 (Fed. Cir. 2018)	27
<i>In re Lee</i> , 277 F.3d 1338 (Fed. Cir. 2002)	12
<i>Innovention Toys LLC v. MGA Entertainment, Inc.</i> , 611 Fed.Appx. 693 (Fed. Cir. 2015).....	12
<i>Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.</i> , 821 F.3d 1359 (Fed. Cir. 2016)	9, 19, 20, 24
<i>International Seaway Trading Corp. v. Walgreens Corp.</i> , 528 F.3d 1233 (Fed. Cir. 2009)	10
<i>Medtronic, Inc. v. Teleflex Life Sci. Ltd. No.</i> 2022-1605, 2024 WL 1208642 (Fed. Cir. 2024).....	23
<i>Mformation Tech. v. Research in Motion Ltd.</i> , 764 F.3d 1392 (Fed. Cir. 2014)	22
<i>SAS Institute Inc. v. Iancu</i> , 138 S.Ct. 1348 (2018).....	6

EXHIBIT LIST	
2001	<i>Orckit Corporation v. Cisco Systems, Inc.</i> , Case No. 2:22-cv-00276, Dkt. No. 46 (E.D. Tex., Jan. 15, 2023), First Amended Docket Control Order (“First Amended Docket Control Order”)
2002	<i>Orckit Corporation v. Cisco Systems, Inc.</i> , Case No. 2:22-cv-00276, Dkt. No. 28 (E.D. Tex., Nov. 4, 2022), Notice of Compliance (“11-4-2022 Notice of Compliance”)
2003	<i>Orckit Corporation v. Cisco Systems, Inc.</i> , Case No. 2:22-cv-00276, Dkt. No. 47 (E.D. Tex., Jan. 19, 2023), Notice of Compliance (“1-19-2023 Notice of Compliance”)
2004	<i>Orckit Corporation v. Cisco Systems, Inc.</i> , Case No. 2:22-cv-00276, Dkt. No. 55 (E.D. Tex., Mar. 23, 2023), Defendant’s Motion To Stay
2005	<i>Orckit Corporation v. Cisco Systems, Inc.</i> , Case No. 2:22-cv-00276, Dkt. No. 56 (E.D. Tex., Mar. 29, 2023), Order Denying Motion to Stay
2006	United States District Courts National Judicial Caseload Profile For the 12 Months Ending March 31, 2023 (available at https://www.uscourts.gov/sites/default/files/data_tables/fcms_na_distprofile0331.2023.pdf) (“Judicial Caseload Statistics”)
2007	<i>Orckit Corporation v. Cisco Systems, Inc.</i> , Case No. 2:22-cv-00276, Dkt. No. 50 (E.D. Tex., Feb. 3, 2023), Notice of Compliance (“2-3-2023 Notice of Compliance”)
2008	Reserved
2009	December 11, 2008 Final Rejection (U.S. Appl. No. 11/123,801) (“’801 Application Final Rejection”)
2010	July 28, 2008 Claim Amendments (U.S. Appl. No. 11/123,801) (“’801 Application Pending Claims”)
2011	<i>Orckit Corporation v. Cisco Systems, Inc.</i> , Case No. 2:22-cv-00276, Dkt. No. 59 (E.D. Tex., Mar. 30, 2023), Order Granting Motion To Amend Invalidity Contentions
2012	<i>Orckit Corporation v. Cisco Systems, Inc.</i> , Case No. 2:22-cv-00276, Dkt. No. 61 (E.D. Tex., April 13, 2023), Order Granting Motion To Amend Invalidity Contentions
2013	“About Orckit-Corrigent: Executive Summary,” 2011

2014	<i>Orckit Corporation v. Cisco Systems, Inc.</i> , Case No. 2:22-cv-00276, (E.D. Tex., April 13, 2023), Defendant’s First Amended Invalidity Contentions (Cover Pleading)
2015	<i>Orckit Corporation v. Cisco Systems, Inc.</i> , Case No. 2:22-cv-00276, (E.D. Tex., April 13, 2023), Defendant’s First Amended Invalidity Contentions (Exhibit A - ’904 Patent Charts)
2016	<i>Orckit Corporation v. Cisco Systems, Inc.</i> , Case No. 2:22-cv-00276, (E.D. Tex., April 13, 2023), Defendant’s First Amended Invalidity Contentions (Exhibit B - ’821 Patent Charts)
2017	<i>Orckit Corporation v. Cisco Systems, Inc.</i> , Case No. 2:22-cv-00276, (E.D. Tex., April 13, 2023), Defendant’s First Amended Invalidity Contentions (Exhibit C - ’740 Patent Charts)
2018	<i>Orckit Corporation v. Cisco Systems, Inc.</i> , Case No. 2:22-cv-00276, (E.D. Tex., April 13, 2023), Defendant’s First Amended Invalidity Contentions (Exhibit D - ’111 Patent Charts)
2019	<i>Orckit Corporation v. Cisco Systems, Inc.</i> , Case No. 2:22-cv-00276, (E.D. Tex., April 13, 2023), Defendant’s First Amended Invalidity Contentions (Exhibit E - Combination Charts)
2020	<i>Orckit Corporation v. Cisco Systems, Inc.</i> , Case No. 2:22-cv-00276, (E.D. Tex., April 13, 2023), Defendant’s First Amended Invalidity Contentions (SME Contentions)
2021	United States District Courts National Judicial Caseload Profile For the 12 Months Ending December 31, 2022 (available at https://www.uscourts.gov/sites/default/files/data_tables/fcms_na_distprofile1231.2022.pdf) (“December 22 Judicial Caseload Statistics”)
2022	Declaration of George Stamatopoulos in support of Patent Owner’s Motion for Pro Hac Vic Admission
2023	Declaration of Michael Ng in support of Patent Owner’s Motion for Pro Hac Vice Admission
2024	Stipulation of Dismissal
2025	Declaration of Miguel Gomez
2026	CV of Michael Gomez
2027	“DPI & DFI: A Malicious Behavior Detection Method Combining Deep Packet Inspection and Deep Flow Inspection” by Guo et al., <i>Procedia Engineering</i> 174, 1309-1314 (2017)

I. INTRODUCTION

Petitioner asserts the challenged claims are obvious in view of Lin and Swenson (“Ground 1”), and Shieh and Swenson (“Ground 2”). The Board should reject both grounds.

Lin and Swenson do not teach the claimed controller, which the Parties agree must at least be capable of controlling deep packet inspection (“DPI”): Lin outsources DPI, and its controller does not support it; Swenson does not disclose DPI (but teaches “deep *flow* inspection” (DFI)); and there is no evidence that a POSITA would combine the two references and adapt their combination to practice the claimed controller with a reasonable expectation of success. Further, Lin uses two criteria for claimed steps that Petitioner admits require a single criterion. The Board should discard Petitioner’s misleading assertions (e.g., that DFI amounts to DPI because flows are series of packets; and flow rules using different criteria operate “in tandem” to produce a single criterion) and reject Ground 1.

The Board should also stand by the Institution Decision’s (Paper 8, “ID”) findings, which the Reply fails to address, and reject Ground 2.

Lastly, because the prior art fails to render obvious the limitations in the dependent claims, the Board should confirm patentability of all challenged claims.

II. CLAIM CONSTRUCTION

The Parties agree that the Board’s analysis remains the same under either proposed construction of “controller.” Paper 31 (“Reply”), 2. The Board thus need not construe “controller” for purposes of a final written decision so long as “controller” is understood to be capable of controlling DPI as required by both constructions. Paper 22 (“POR”), 17.

III. THE CHALLENGED CLAIMS ARE PATENTABLE

A. Ground 1: Lin and Swenson do not render the claims obvious.

As explained below, Lin’s controller does not support DPI, Swenson does not disclose DPI, and there is no support that a POSITA would combine Lin and Swenson to practice the claimed controller.

1. Lin does not teach the claimed controller.

As Petitioner concedes, “Lin discusses a separate security service” for DPI (Reply, 4) and thus does not disclose the claimed controller.

The record also disproves Petitioner’s assertion that a POSITA would have implemented Lin’s security service in the controller as “one of the limited number of design options.” Reply, 4, 7.

First, Lin teaches using its controller exclusively for network administration and expressly outsources security (e.g., firewalls, “DPI”) to external “security

vendors.” Ex1005, 3:11-24. The controller and security service are separate in all of Lin’s embodiments:

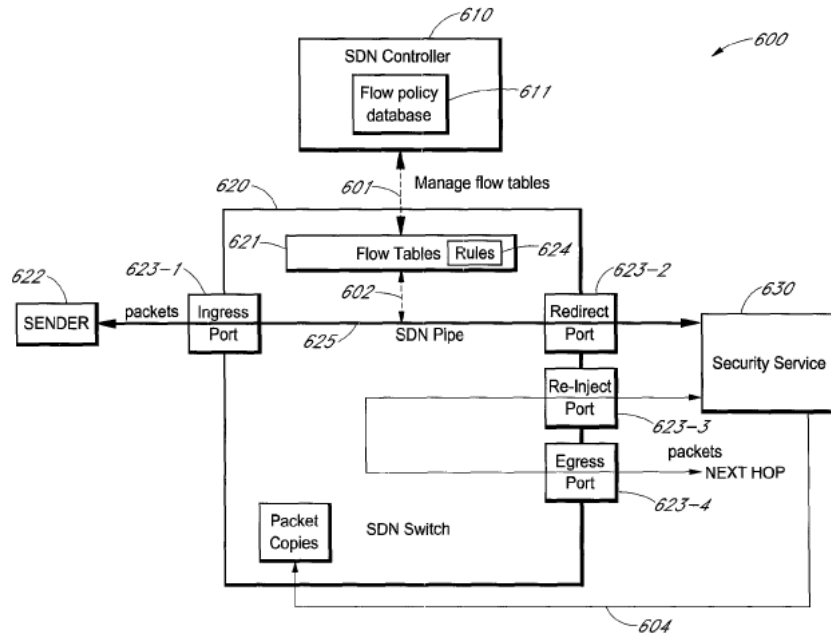


FIG. 6

Using the controller for security is thus not an “option” in Lin, which is directed to creating a “pipe” connecting a switch to a security service. *Id.*, Title, Abstract.

Second, as taught in the ’111 Patent, the only controller disclosed in Lin (the “OpenFlow” controller) (Ex1005, 3:45-52) does not support DPI:

[T]he OpenFlow protocol allows addition of programmability to network nodes for ... packets-processing operations under the control of the central controller, [but] ***OpenFlow does not support any mechanism to allow DPI of packets through the various networking layers as defined by the OSI model.*** Specifically, the current OpenFlow specification defines a

mechanism to parse and extract only packet headers, in layer-2 through layer-4, from packets flowing via the network nodes. *The OpenFlow specification does not define or suggest any mechanism to extract non-generic, uncommon, and/or arbitrary data patterns contained in layer-4 to layer 7 fields. In addition, the OpenFlow specification does not define or suggest any mechanism to inspect or to extract content from packets belonging to a specific flow or session.* This is a major limitation as it would not require inspection of the packet for the purpose of identification of, for example, security threats detection.

Ex1001, 1:50-67.² A POSITA would thus *need* a separate security service for DPI and *could not opt* to use Lin’s controller. *See* Ex2025, ¶¶52-55.³

Third, Petitioner incorrectly asserts that Mr. Gomez’s opinion that “security services were not normally combined with a controller” and that doing so “would be

² Unless otherwise noted all emphases are added.

³ Petitioner argues that the security service “may share certain common technical characteristics with the controller” (e.g., connections, etc.), and packets must be routed to the security service. Reply, 4-6. These commonplace characteristics do not show that a POSITA could support DPI in a controller, particularly since controllers like Lin’s did not support DPI. Ex2025, ¶¶54-55.

prohibitively expensive to implement as part of the controller” is unsupported. Ex2025, ¶55; Reply, 6-7. For example, the ’111 patent explains that using the controller for DPI was known to be inefficient, costly, and problematic, as of the priority date:

The straightforward approach of *routing all traffic ... to the central controller introduces some significant drawbacks, such as increased end-to-end traffic delays between the client and the server; overflowing the controller capability to perform other networking functions; and a single point of failure for the re-routed traffic*. Therefore, it would be advantageous to provide a solution that overcomes the deficiencies noted above and allow efficient DPI in SDNs.

Ex1001, 2:1-10. Accordingly, contrary to Petitioner’s assertion that there is no such evidence (Reply, 6-7)—and *consistent* with Mr. Gomez’s testimony—the record is clear that controllers did not support DPI as of the priority date and using them for DPI against the conventional wisdom was inefficient and costly. The record, including Lin (which discloses no rationale for adapting its controller to support DPI), thus contradicts Petitioner’s contentions that using the controller for DPI was straightforward or obvious.

Petitioner asserts that a POSITA would find it trivial to integrate Lin’s security service in the controller as “one component” because Swenson uses conventional

components for security. Reply, 6-7. To the extent that Petitioner is attempting to construe “controller” as “one component” for performing DPI and controlling a network, the Board should reject such a construction as untimely because it was not raised in the Petition. *SAS Institute Inc. v. Iancu*, 138 S.Ct. 1348, 1351 (2018). Further, as discussed below, Swenson does not disclose DPI, let alone in a controller with conventional components.

Petitioner also incorrectly asserts that the problems disclosed in the ’111 patent with respect to using the controller for DPI did not plague Lin because it routed only “specific packets to the security device.” Reply, 5-6. Lin expressly discloses (i) that “[r]e-injecting packets that pass inspection consume[s] bandwidth” and (ii) mitigation techniques for this issue. Ex1005, 7:10-23. A POSITA would thus understand that Lin faced the same constraints and impediments to using the controller for DPI as disclosed in the ’111 patent. Further, a POSITA would understand that skipping DPI with Lin’s “bypass flow rules” was the exception to redirecting packets for inspection, not the default rule, as Petitioner asserts. *Id.*, 7:23-27. In any event, Lin does not disclose that the “bypass flow rules” make it possible, let alone efficient, to use the controller for DPI. Nor does Lin disclose the use of only one security device, such that the security device would be a “single point of failure” just like the controller as Petitioner asserts. Reply, 6. The record

thus contradicts Petitioner's assertion that a POSITA would not expect Lin to face the problems described in the '111 patent.

Accordingly, (including for reasons pertaining to Swenson *infra*) Lin does not teach or render obvious the claimed controller.

2. Swenson discloses deep flow inspection, not deep packet inspection or the claimed controller.

Petitioner's contention that Swenson teaches the claimed controller boils down to whether Deep ***Packet*** Inspection (DPI)—*i.e.*, the well-known technique in the '111 patent that Swenson nowhere mentions—is the same as Deep ***Flow*** Inspection (DFI), a different data monitoring technique discussed in Swenson. It is not.

The record contradicts Petitioner's assertion that DFI is the same as DPI because a “flow” is a series of packets, and Swenson discloses inspecting the “response payload of a HTTP packet.” Reply, 7-8.

As a threshold matter, though a flow is a series of packets, inspecting a flow is not the same as inspecting individual packets. Petitioner does not dispute Mr. Gomez's testimony that DPI was a well-known technique for performing a “thorough inspection process” directed to the payload of a packet, “capable of looking at Layer 2 and beyond Layer 3 of the OSI model .. up to Layer 7,” and “offer[ing] control of network traffic that goes beyond classification of packets.”

Owing to its thoroughness, the fine-grain DPI had limitations, including “less visibility into the overall traffic patterns of networks” and higher processing power requirements. Ex2025, ¶¶57-59.

Mr. Gomez also testified that: (i) DFI is used to inspect flows (rather than individual packets) to glean network information (including IP addresses, ports, protocol types, traffic metrics, and state information) that is not conveyed by or ascertainable by inspecting individual packets, (ii) the two techniques have different capabilities and technical challenges, and (iii) Swenson’s disclosure of DFI for among other things “collection of statistic information” and bandwidth monitoring reinforced a POSITA’s understanding that DFI was used to inspect flows, not individual packets. *Id.* ¶¶60-65.

His testimony that DPI and DFI are different is further supported by at least one academic article discussing combining the “fine-grain DPI with the coarse-grain DFI” in a single method for “malicious behavior detection,” thus demonstrating that the two are different. Ex1016, 106; Ex2027 (discussing DFI and DPI as two different techniques).

Mr. Gomez’s testimony is thus supported by: (i) the different terms of art used for the two techniques, (ii) Swenson’s disclosure of DFI functionalities that are not performed with DPI, (iii) Lin’s disclosure of outsourcing DPI to a dedicated security

service, (iv) extrinsic evidence distinguishing between DPI and DFI, and (iv) his own experience.

In contrast, Petitioner asserts (incorrectly and transparently oversimplifying things) that a “flow is a series of packets,” and Swenson’s DFI includes inspection of a HTTP request/response payload. Reply, 7-11. The Board should reject this assertion.

First, that a flow is a series of packets only proves that a POSITA would know that (i) a flow is *not* an individual packet and (ii) Swenson’s use of coarse-grained DFI, as opposed to fine-grained DPI, is directed to high-level information about traffic metrics, not deep packet inspection.

Second, Swenson nowhere teaches that a HTTP request/response payload is an *individual packet payload*. The Board should reject Petitioner’s assertion that such a request can be embodied in a single packet. Reply at 11. As a threshold matter, the Petition did not raise this argument, and it is thus untimely. Reply, 13 (raising argument for first time). *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1367 (Fed. Cir. 2016) (declining to address new reply arguments and emphasizing “importance that petitioners ... adhere to the requirement that the initial petition identify ‘with particularity’ the ‘evidence that supports the grounds for the challenge to each claim’”). Moreover, Swenson does

not teach such an embodiment; and Petitioner has failed to argue—let alone provide evidence showing—*that a POSITA would understand* such a single-packet HTTP response/request embodiment is possible. Obviousness is determined from the perspective of a POSITA. *E.g., International Seaway Trading Corp. v. Walgreens Corp.*, 528 F.3d 1233, 1244 (Fed. Cir. 2009) (“Obviousness, like anticipation, requires courts to consider the perspective of the ordinary observer.”). Swenson does not disclose a single-packet embodiment, and there is no evidence that a POSITA would understand Swenson to disclose one. The Board should thus reject Petitioner’s assertion. In any event, a POSITA would understand HTTP requests/responses to refer to flows, not individual packets. Ex2025, ¶¶69.

Third, even assuming a POSITA understood a HTTP request/response could be embodied in a single packet, Swenson’s inspection still would not amount to DPI. Mr. Gomez testified and the ’111 patent teaches that DPI has a number of characteristics and capabilities beyond inspecting a single packet payload. *Id.* ¶¶58-59; Ex1001, 1:21-29. In contrast, Swenson discloses inspecting an HTTP request/response as a limited precursor step for performing DFI. Ex1007, ¶[0065] (describing “send[ing] ... ICAP request message ... comprising the HTTP GET request header and a portion of the response payload to the network controller 140, which inspects the message *to determine whether to monitor the flow or optimize*

the video.”). Thus, even if Swenson disclosed inspecting a single packet payload (it does not), a POSITA understand this is not DPI.⁴

Fourth, Swenson consistently uses “payload” in connection with flows, not single packets and teaches “selectively inspect[ing] user flows of interest” in contrast to “conventional inline TCP throughput monitoring devices that monitor every single data packet transmitted and received[.]” Ex1007, ¶¶[0028], [0061], [0064], [0078]. A POSITA would thus understand that Swenson’s DFI inspects flow information, not individual packets.

Accordingly, Swenson does not teach or render obvious the claimed controller.

3. A POSITA would not combine/adapt Lin and Swenson to practice the claimed controller.

The Federal Circuit has held that proving obviousness requires articulating a motivation for which a POSITA would combine prior art references, supported by adequate evidence, and an express and rational connection of the POSITA’s

⁴ Petitioner has not proposed construing DPI, let alone construing it as simply inspecting a packet payload, nor contended that a POSITA would understand DPI as the inspection of a packet payload.

motivation with the evidence presented. *See, In re Lee*, 277 F.3d 1338, 1343-45 (Fed. Cir. 2002) (conclusory statements are insufficient); *Cutsforth v. MotivePower*, 636 Fed.Appx. 575, 578 (Fed. Cir. 2016) (must positively explain motivation); and *Arendi v. Apple*, 832 F.3d 1355, 1361-62 (Fed. Cir. 2016) (“common knowledge or common sense” insufficient to find motivation). Petitioner’s contention that a POSA would combine Lin and Swenson to increase efficiency and conservation in operating network systems fails to meet this standard. Reply, 11.

Petitioner asserts that the Lin/Swenson combination would have made “common sense” to a POSITA because of these purported benefits but fails to articulate or provide evidence showing *why* a POSITA would (i) understand that combining Lin and Swenson would increase efficiency and resource conservation and (ii) reasonably expect that it could successfully combine Lin and Swenson to practice the claimed controller. *Innovation Toys LLC v. MGA Entertainment, Inc.*, 611 Fed.Appx. 693, 698 (Fed. Cir. 2015) (“the testimony gives little reason that a person of ordinary skill in the art—with [the prior art references] hanging somewhere on the figurative wall of pertinent art, as we previously held—would have defined a problem to be solved in such a way as to provide a motivation to pick out those references for combination.”)

The crux of Petitioner’s argument is that a POSITA would have found it obvious to implement security processing in Lin’s controller in light of Swenson because **(a)** Lin and Swenson share generic similarities (e.g., a central controller, packet routing, and different forms of data inspection) and **(b)** determining “which packets to redirect ... increases the efficient operation of a computer network.” Reply, 11 (citing Paper 1 (“Petition”), 20-25). There are several problems with this argument.

First, even assuming that Swenson taught DPI (it does not), there is no evidence (including in Swenson) that using the controller for DPI is efficient. Swenson teaches against sending packets to the controller and instead discloses selective flow monitoring. Ex1007, ¶[0028] (“In contrast to conventional inline TCP throughput monitoring devices that monitor every single data packets transmitted and received, *the network controller 140* is an “out-of-band” computer server that *interfaces with the steering device 130 to selectively inspect user flows of interest.*”). Likewise, Lin teaches outsourcing DPI. *Supra*, III.A.1. Petitioner’s argument that combining Lin/Swenson would produce efficiency thus lacks evidentiary support (including as to *why* a POSITA would believe that this specific combination would be efficient) and fails for this reason.

Second, Lin teaches (i) a controller that does not support DPI, (ii) outsourcing DPI, (iii) that transmitting packets for inspection consumes bandwidth, and (iv) using optimization techniques to avoid burdening the network with packet inspection (e.g., locally copying packets and sending only an index of inspection results). *Supra*, III.A.1; Ex1005, 7:10-22. Contrary to Petitioner’s assertion, a POSITA would thus understand that sending packets to the controller or using the controller for DPI is inefficient.

Third, Swenson does not disclose DPI (or the claimed controller), and Lin’s controller does not support DPI. *Supra* III.A.1-2. A POSITA would thus understand that practicing the claimed controller would require adapting the combined Lin/Swenson controller to include functionalities beyond those found in prior art controllers. There is no evidence that a POSITA would be motivated to make or adapt such a combination or could reasonably expect to do so successfully.

The remainder of Petitioner’s assertions (Reply, 12-13) likewise fail.

First, “certain network flows” are *not* “directed to the controller for DPI” (Reply, 12), since Swenson teaches DFI—not DPI—and more broadly against monitoring individual packets. *Supra*, 12; Ex1007, ¶[0028]. Second, there is no basis the assertion that “a POSA would have understood that Swenson could analyze packets for a security function” (Reply, 12) because Swenson teaches against

individual packet monitoring and in its sole mention of security functions (which Swenson does not describe Ex1007, ¶[0039]), Swenson mentions only “conventional components” that—as discussed with respect to Lin—did not support DPI in the controller. Ex1007, ¶[0039]; *supra* at III.A.1-2. Third, contrary to Petitioner’s assertion that there is no evidence DPI is more taxing than DFI (Reply, 12), Mr. Gomez explained why DFI is less taxing on the controller (e.g., Ex2025, ¶¶59, 62 (DPI is a detailed inspection technique that “requires significant processing power and may struggle with high-bandwidth networks or encrypted traffic” while DFI “focuses on broader patterns”)), consistent with Lin’s teaching about bandwidth consumption (Ex1005, 7:10-22) and Swenson’s teaching that the controller “selectively inspect[s] user flows” rather than individual packets. Ex1007, ¶[0028]. Further, Swenson and Lin do not compare DPI and DFI with respect to the controller (Reply, 12) because ***neither performs DPI at the controller***, and there is no evidence that Swenson’s DFI (unlike DPI) is “taxing” on the controller. Fourth, Petitioner’s untimely assertion that a HTTP request/response can be embodied in a single packet is addressed *supra* at III.A.2. Fifth, Petitioner’s assertion that Swenson’s conventional security components are part of the controller (Reply, 13) fails because conventional controllers at the time of the invention (e.g., Lin) could not support DPI (*supra*, III.A.1); thus, Swenson’s mention of “conventional components” in a

controller does not teach the claimed controller. Sixth, Petitioner’s assertion that prior art “drawbacks” did not apply to Lin is addressed *supra* at III.A.1. And, seventh, Petitioner’s assertion that a POSITA could expect to successfully place “the security service in the controller just as if it was a separate module” fails because, as discussed *supra* at III.A.1, it is predicated upon an untimely new construction and, in any event, contrary to the record (e.g., Swenson does not perform DPI, Lin’s controller does not support DPI, and the ’111 patent teaches that state-of-the-art OpenFlow controllers did not support DPI, *supra*, III.A.1-2).

Accordingly, the Board should reject Petitioner’s contention that a POSITA would be motivated to combine Lin and Swenson with a reasonable expectation of success.

4. Lin does not teach sending the packet to the second entity or a different entity responsive to a single criterion.

Claim 1 recites: “responsive to the packet *not satisfying* the criterion, *sending*...the packet to the second entity” [1.5], and “responsive to the packet *satisfying* the criterion, *sending* the packet ... to an entity ... other than the second entity” [1.6]. Petition, 30-32. Petitioner does not dispute that both claimed steps are responsive to the same criterion.

In contrast, Lin on its face teaches two criteria: one criterion for sending a packet to a second entity, and a different criterion for sending a packet to another

entity. POR, 39-42. Petitioner admits that Lin’s Table 3 a “bypass flow rule” and a “redirect flow rule” for performing two functions: *bypassing* the security service or *redirecting to* the security service. The POR does not assert that these rules are themselves criteria (Reply, 15) but explains that each rule uses a different criterion. Petitioner admits that Lin’s two rules contain packet-applicable criteria. *Id.* (“instead the flow rules contain packet-applicable criterion [*sic*]”). The criteria in Lin’s two rules are shown in Petitioner’s annotated Table 3:

TABLE 3							
IN_PORT	...	IP src	TCP src port	TCP dst port	...	Action	Count
Ingress_port_ID	*	*	*	80	*	Redirect port	10
Redirect_port_ID	*	*	80	*	*	Ingress port	10
Ingress_port_ID	*	*	*	*	*	Egress port	130
Egress_port_ID	*	*	*	*	*	Ingress port	130

Table 3 of Lin (Annotated)

TABLE 3							
IN_PORT	...	IP src	TCP src port	TCP dst port	...	Action	Count
Ingress_port_ID	*	*	*	80	*	Redirect port	10
Redirect_port_ID	*	*	80	*	*	Ingress port	10
Ingress_port_ID	*	*	*	*	*	Egress port	130
Egress_port_ID	*	*	*	*	*	Ingress port	130

Table 3 of Lin (Annotated)

The top two rows redirect packets to the security service if a first criterion is satisfied (port 80 is the destination/source port); and the bottom two rows bypass the security service if a second criterion is satisfied (no TCP source or destination port indicated). There is no evidence that a POSITA would understand these two criteria are one and the same criterion. Indeed, as discussed in the POR (*and not addressed in the Reply*), Lin does not teach how a packet is sent if either the bypass or redirect flow rule criteria are both not satisfied. POR, 41.

In any event, Petitioner admits that Lin uses more than one condition to route its packets. Reply, 15-16 (“*these conditions determine* whether or not the packet is forwarded to the security service”), (“Lin states, ‘When *the conditions* are met’”). Likewise, Petitioner identifies as a different criterion each of the “one or more conditions used [in Lin] to identify particular packets for inspection” (Petition, 29-30) and states that each of those conditions (e.g., ‘IN_PORT’; ‘MAC src’; ‘MAC dst’; ‘IP src’; ‘IP dst’) are “examples of the criterion applicable to a particular packet.” Petition, 26.

To sidestep Lin’s disclosure of separate flow rules with separate criteria, Petitioner asserts that the flow rules “operate in tandem to decide what to do with a packet.” Rep, 16. This assertion is untimely and should be rejected, *Intelligent Bio-Sys., Inc.*, 821 F.3d at 1367 (declining to address new reply arguments not raised in

petition); and it only shows that Lin teaches using separate criteria and rules—*in tandem*—to route packets. It does not show that Lin uses a single criterion or that this would be a POSITA’s understanding of Lin.⁵

Accordingly, because Petitioner has failed to prove that Lin teaches using a single criterion, as required by all challenged claims, the Board should find the claims patentable.

⁵ Petitioner also argues for the first time in the Reply that “[i]f the single criterion indicates that the packet is an HTTP packet, then the packet is redirected to the security service [and this] embodiment accounts for all packets ...[.]” Reply, 16. Though this argument suffers from the same flaws as Petitioner’s other arguments about Table 3, the Board should reject it as untimely raised for the first time in the Reply, addressing portions of Swenson for the first time. *Ariosa Diagnostics v. Verinata Health, Inc.*, 805 F.3d 1359, 1367 (Fed. Cir. 2015) (declining to address reply arguments discussing “previously unidentified portions of a prior-art reference to make a meaningfully distinct contention”); *Intelligent Bio-Sys., Inc.*, 821 F.3d at 1367.

B. Ground 2: Shieh and Swenson do not render the claims obvious

The ID found that Petitioner failed to explain “how identification of ‘TCP FIN or TCP RST packets’ corresponds to the teachings surrounding filtering rules in Shieh;” “Shieh does not appear to teach what happens to a packet [when] a TCP FIN or TCP RST packet is identified;” and “Shieh discloses that packet destinations are determined by the bypass flag—which is separate from the TCP FIN or TCP RST packet.” ID, 19. The Reply does not address these findings; thus, the Board should reject Ground 2.

As an initial matter, the Board should reject Petitioner’s assertion that the value of Shieh’s bypass flag is a packet-applicable criterion responsive to which the network access device forwards a packet to the security device. Reply, 16-17, 19. The Petition only identifies Shieh’s “TCP FIN or TCP RST packets” as the packet-applicable criterion, not the bypass flag, failing to “explain how” the two are related. Petition, 62-63; ID, 19. The Board should thus reject Petitioner’s argument that the bypass flag is the packet-applicable criterion as untimely. *Ariosa*, 805 F.3d at 1367; *Intelligent Bio-Sys., Inc.*, 821 F.3d at 1367. But even if the Board considers Petitioner’s untimely argument, Shie’s bypass flag is not “sen[t] by the controller to the network node” (as required by claim 1). Shieh discloses that the bypass flag is sent by the **security device** (Ex1006, [0030]), which the Petition maps to the claimed

“entity that is included in the instruction and is other than the second entity,” not the claimed controller (which the Petition maps to “Controller 208”). Petition, 57. Accordingly, Petitioner’s argument fails in any event because Shieh fails to disclose sending the claimed criterion by the controller as claimed.

Petitioner also incorrectly asserts that “the controller communicates to the network access devices to use the ‘identification of TCP FIN or TCP RST packets’ as a packet applicable criterion to decide whether to send packets to a security service for inspection.” Reply, 17-18. Petitioner appears to suggest that the identification of TCP FIN or TCP RST packets are part of filtering rules that forward a packet. Not so. Shieh does not disclose that “identification of TCP FIN or TCP RST packets” determines the destination of a packet. Ex1006, [0036]. Shieh merely states that the receipt of a TCP FIN or TCP TST packet is a “special event” that the I/O function notifies the security-processing function of. *Id.* As the ID already found, “Shieh does not appear to teach what happens to a packet in a special even such as a TCP FIN or TCP RST packet is identified.” ID, 19. There is no disclosed connection between the process of identifying TCP FIN or TCP TST packets for a special event described in paragraph 36 and the process of forwarding packets based on a set bypass flag described in paragraph 37. Ex1007, ¶¶[0036]-[0037]. And to be clear, the TCP FIN or TCP RST packets are **not** sent from the controller; instead,

Shieh discloses that TCP FIN or TCP TST packets are sent by the network source node and received by the network switch as part of the “packet stream,=.” Ex1006, 36. There is also no teaching in Shieh or elsewhere motivating a POSITA to modify Shieh’s controller to send the TCP FIN or TCP RST packets, nor did the Petition explain how or why a POSITA would modify Shieh in this manner. Likewise, nothing in the record explains why a TCP FIN or TCP TST packet would originate from the controller as in Petitioner’s proposed modification rather than Shieh’s source node.

Finally, the Reply asserts that Shieh’s TCP FIN or TCP TST packets determine a packet’s destination. Reply, 18. Not so. As the ID found, a bypass flag—not the separate TCP FIN or TCP TST packets—routes packets to Shieh’s security device. ID, 19. The Reply fails to provide any basis to overturn that finding.

Accordingly, the Board should maintain the ID’s determinations concerning Shieh and Swenson.

C. Claims 3-5

Claims 1 and 3 recite steps that must be performed in the order written. POR, 46-47; *Mformation Tech. v. Research in Motion Ltd.*, 764 F.3d 1392, 1398-99 (Fed. Cir. 2014) (claim language “requires that the steps be performed in the order written”); *see also Medtronic, Inc. v. Teleflex Life Scis. Ltd.*, No. 2022-1605, 2024

WL 1208642 at *5 (Fed. Cir. Mar. 21, 2024). The Petition fails to allege that Lin teaches the additional steps of claim 3 after the steps of claim 1. POR, 46-48. The Reply fails to address this deficiency, asserting instead that “PO has not explained what requires the steps to be performed in order.” Reply, 19.

The POR explained the steps that need to be performed. POR, 46-47; Ex2025, 91-92. Petitioner asserts that claim 3 narrows the last step in claim 1; thus, Lin thus satisfies claim 3 by disclosing “mirroring.” Reply, 19-20. Not so. Claim 3 *adds* a step after the last step of claim 1, which Lin does not disclose. POR, 46-49. Petitioner’s arguments as to claim 3 fail, as do those for claims 4-5 for the same reasons.

D. Claim 6

Petitioner conflates flows with packets to assert that Swenson stores packets in memory (including by incorrectly asserting that “PO admits a flow is stored in the cache memory 322”) (Reply, 20); but flows and flow data are not the same as packets. Ex2025, ¶¶98-99. Further, the POR explains that Swenson discloses storing flow cache entries consisting of a list of flows and flow statistics, not individual packets as required by the claim. POR, 50-52.

Petitioner’s contention that Swenson discloses storing a packet portion because its flow cache memory stores “source IP 722” and “cookie 744” (Reply, 20-

21) likewise fails. First, this argument was not presented in the Petition, which nowhere identifies “cookie 744” as a portion of a packet, let alone one stored in memory (*see* Petition, 39-40); thus, the Board should not consider it. *Ariosa Diagnostics*, 805 F.3d at 1367; *Intelligent Bio-Sys., Inc.*, 821 F.3d at 1367.

Second, Petitioner fails show that “source IP 722” or “cookie 744” are portions of a packet. Swenson’s Figure 7 only shows that element 722 is stored in flow cache block 720, and element 744 is stored in flow statistics block 740:

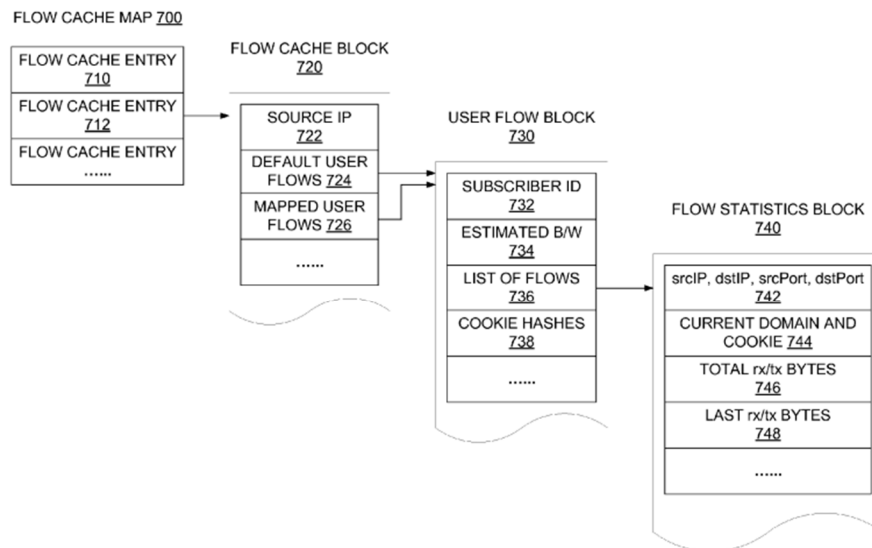


FIG. 7

Ex1007, Fig. 7. There is thus no support in Swenson that elements 722 or 744 are portions of a packet or originated from a packet.

Third, Petitioner also asserts that a memory can store an IP address, MAC address, or TCP source port (Reply, 21) but fails to adduce evidence that these are

portions of a packet. Further, Swenson discloses that the “source IP address, MAC address, subscriber ID, or other identifier” are used to create hash indices to retrieve flow entries. Ex1007, ¶¶[0073]. Thus, even assuming these values were portions of a packet, hashing transforms them such that they are no longer a portion of a packet. In addition, Swenson uses the hash as an index (i.e., address) to retrieve a flow entry and does not state that the hash itself is stored. Ex1007, ¶¶[0073], [0046].

Accordingly, Petitioner fails to demonstrate that Swenson suggests storing any portion of a packet.

E. Claim 7

Claim 7 requires “sending a portion of the packet” and is distinguished from its parent claim 5—which recites “sending the packet or a portion thereof”—because it unambiguously requires sending less than a whole packet. Ex1001, claims 5, 7; *Aspex Eyewear, Inc. v. Marchon Eyewear, Inc.*, 672 F.3d 1335, 1348 (Fed. Cir. 2012) (limitation in dependent claim presumptively not duplicative of parent claim limitations). The specification discloses embodiments consistent with claim 7, in which network nodes are “configured to extract and send only a portion of a packet data that contains meaningful information.” Ex1001, 4:20-22.

Contrary to Petitioner’s assertion that sending portions of HTTP requests/responses satisfies claim 7, Swenson nowhere teaches that its HTTP

responses/requests are packets (or that portions of those requests are portions of packets). *Supra*, III.A.2; POR, 52-54. As discussed in the POR (*id.*, 52-54), a single HTTP request comprises multiple packets; thus, a POSITA would not understand a portion of such a request to be the claimed packet portion.

The remainder of Petitioner’s arguments (i.e., “[a] HTTP response can be encompassed within a single packet,” “Swenson could choose to forward only a portion of multiple response packets”) have no support in Swenson and are unfounded speculation, as Swenson does not disclose sending only a single packet, nor did the Petition allege that a POSITA would reach such an understanding from Swenson’s disclosure. Accordingly, as discussed *supra* at III.A.2, the Board should reject them.

F. Claim 16

There is no evidence that claim 16 is obvious. Even crediting the Reply’s contentions that a “packet includes distinct header and payload fields” and a “header field includes one or more flag bits” (Reply, 23), it does not follow—and there is no supporting evidence—that a POSITA would understand the “packet-applicable criterion is that one or more of the flag bits is set,” as required by claim 16. Having failed to identify this missing limitation in the prior art, Petitioner relies only on expert “say-so” to assert that a POSITA would have known that “flag bits ... serv[e]

as packet applicable criterion.” Bare assertions as to a POSITA’s understanding, however, are not the “reasoned analysis and evidentiary support” needed under the “searching” standard for supplying a missing limitation. *See DSS Tech. Mgmt. Inc. v. Apple Inc.*, 885 F.3d 1367, 1377 (Fed. Cir. 2018) (The Board may not “rel[y] on ‘ordinary creativity’ ‘as a wholesale substitute for reasoned analysis and evidentiary support’ ‘when dealing with a limitation missing from the prior art references specified’”); *Arendi SARL v. Apple Inc.*, 832 F.3d 1355, 1362-63 (Fed. Cir. 2016) (“In cases in which ‘common sense’ is used to supply a missing limitation, as distinct from a motivation to combine, moreover, our search for a reasoned basis for resort to common sense must be searching.”). Accordingly, the Board should reject Petitioner’s challenge with respect to claim 16.

G. Claim 30

Petitioner does not dispute that claim 30 adds steps to those in claim 1 (“receiving,” “checking,” and “sending”) that are performed on “additional” packets, *i.e.*, different than the packet of claim 1.

Petitioner concedes that Lin’s and Swenson’s disclosures in the Reply do not suggest performing steps on “one or more additional packets” but wrongly asserts PO “reads too much” into them. Reply, 23. These disclosures show that Lin and Shieh ***do not*** route additional packets based on a claimed “criterion” and thus

contradict Petitioner's assertion that "the methods of Lin and Shieh can be applied to additional packets." *Id.*; *also* POR, 57-59. Petitioner has not identified disclosures in Lin and Swenson that suggest sending "one or more additional packets" based on the claimed "criterion." Thus, the Board should confirm claim 30 is patentable.

IV. CONCLUSION

For the reasons above, PO respectfully requests that the Board find the challenged claims patentable.

Date: May 24, 2024

Respectfully submitted,

/Minghui Yang/
Minghui Yang
Reg. No. 71,989
Counsel for Patent Owner
CARMICHAEL IP, PLLC
8607 Westwood Center Drive
Suite 270
Tysons, VA 22182
Email: mitch@carmichaelip.com
Telephone: (703) 646-9248

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITS

This Patent Owner's Sur-Reply ("Sur-Reply") consists of 5,592 words, excluding table of contents, table of authorities, certificate of service, this certificate, or table of exhibits. The Sur-Reply complies with the type-volume limitation of 5,600 words as mandated in 37 C.F.R. § 42.24. In preparing this certificate, counsel has relied on the word count of the word-processing system used to prepare the paper (Microsoft Word).

Dated: May 24, 2024

/Minghui Yang/
Minghui Yang
Counsel for Patent Owner

CERTIFICATE OF SERVICE

The undersigned hereby certifies that the following document was served by electronic service, by agreement between the parties, on the date below:

PATENT OWNER'S SUR-REPLY

The names and email addresses of the parties being served are as follows:

Jeffrey D. Blake jblake@merchantgould.com
Andrew J. Lagatta alagatta@merchantgould.com
OrckitIPR@merchantgould.com

Kyle Tsui kyle.tsui@fischllp.com
Andrew Ramos andrew.ramos@fischllp.com
ipr@fischllp.com

Respectfully submitted,

/Minghui Yang/

Date: May 24, 2024